RSA Public Key Cryptography

(Rivest, Shamir, Adleman 1977. Cocks 1974)

Suppose

- N letter alphabet (e.g. $N = 26$)
- k-letter plaintext message units

(e.g. $k = 3$

MEET_ME_TONIGHT

MEE, T_M, E_T, ONI, GHT)

- l-letter ciphertext message units

(e.g. $l = 4$

XYAUVX2W

XYAU, VXZW)

Plaintext message units $\longleftrightarrow$ Integers in range $0 \le i \le N^k - 1$

Ciphertext message units $\longleftrightarrow$ Integers in range $0 \le i \le N^l - 1$

Cryptosystem

- Each user chooses two distinct random prime numbers p and q (of around 1000 digits each, to be safe with modern technology)
- choose an integer e with with $\gcd(e, p-1) = 1 = \gcd(e, q-1)$.
- Each user computes

$$n = pq$$

and publishes the enciphering key

$$K_E = (n, e).$$

- Each user computes (using the Euclidean algorithm)

$$d = e^{-1} \bmod \phi(n)$$

where $\phi(n) = (p-1)(q-1)$.

- The deciphering key

$$K_D = (n, d)$$

is kept secret.

- The enciphering function is

$$f_{(n,e)} : \mathbb{Z}_n \to \mathbb{Z}_n, \; x \longmapsto x^e \bmod n$$

- The deciphering function is

$$f_{(n,d)} : \mathbb{Z}_n \to \mathbb{Z}_n, \; x \longmapsto x^d \bmod n$$

Lemma

$$(x^e)^d \equiv x \bmod n$$

Example of an RSA cryptosystem

26-letter alphabet $A=0, B=1, \dots, Z=25$

$k=3$: 3-letter plaintext message units

$l=4$: 4-letter ciphertext " "

I want to send Alice the message

YES

Alice's public key is found on her web page to be

$$K_E^{Alice} = (n, e) = (46927, 39423)$$

$$YES \longleftrightarrow 24 \cdot 26^2 + 4 \cdot 26 + 18 \cdot 26^0$$

$$= 16346$$

$$f^{Alice}_{(n,e)}(YES) = 16346^{39423} \mod 46927$$

$$= 21166$$

$$21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 \cdot 1$$

$$= BFIC$$

I send Alice the enciphered message

BFIC.

Remark 1 It is believed that the computation of d from (n, e) necessitates the factorization of $n = pq$.

Remark 2 It is believed that (with current technology) the factorization would take a prohibitively long time.